ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 15843.2—2024
代替 GB/T 15843.2—2017

网络安全技术　实体鉴别
第2部分：采用鉴别式加密的机制

Cybersecurity technology—Entity authentication—Part 2：Mechanisms using authenticated encryption

（ISO/IEC 9798-2：2019，IT Security techniques—Entity authentication—Part 2：Mechanisms using authenticated encryption，MOD）

2024-09-29 发布　　2025-04-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是GB/T 15843的第2部分。GB/T 15843已经发布了以下部分：

——信息技术　安全技术　实体鉴别　第1部分：总则；

——网络安全技术　实体鉴别　第2部分：采用鉴别式加密的机制；

——信息技术　安全技术　实体鉴别　第3部分：采用数字签名技术的机制；

——网络安全技术　实体鉴别　第4部分：采用密码校验函数的机制；

——信息技术　安全技术　实体鉴别　第5部分：使用零知识技术的机制；

——信息技术　安全技术　实体鉴别　第6部分：采用人工数据传递的机制。

本文件代替GB/T 15843.2—2017《信息技术　安全技术　实体鉴别　第2部分：采用对称加密算法的机制》，与GB/T 15843.2—2017相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 增加了标准适用范围和适用对象的描述，删除了“范围”中关于时变参数、信息传递次数的说明，将其纳入第5章（见第5章，2017年版的第1章）；

b) 增加了术语“验证方”及其定义（见3.3），更改了术语“可鉴别的加密”为“鉴别式加密”（见3.1，2017年版的3.1）、“时间戳”（见3.4，2017年版的3.6）、“声称方”（见3.2，2017年版的3.3）、“可信第三方”（见3.5，2017年版的3.7），删除了术语“密文”“消息鉴别码”“消息鉴别码算法”（见2017年版的3.2、3.4及3.5）；

c) 增加了符号“SID_m^i”（见第4章、第6章、第7章、第8章及附录A），增加了缩略语“DER”“MAC”（见4.2）；

d) 增加了“通则”，将鉴别机制中与时变参数、信息传递次数等相关的说明内容纳入此部分，同时补充了对附录的说明（见第5章）；

e) 将“要求”中“对称加密”更改为“鉴别式加密”并修改了表述（见第6章，2017年版的第5章）；

f) 增加了初始化向量的相关要求（见第6章）；

g) 将“可信第三方”更改为“在线可信第三方”并修改了表述（见第7章及第8章，2017年版的第6章及第7章）；

h) 将各类机制的标识符，由数字更改为英文缩写（见第4章、第7章、第8章、附录A，2017年版的第6章、第7章、附录A）；

i) 更改了“对象标识符”（见附录A，2017年版的附录A），删除了“符合ASN.1基本编码规则（BER）的编码示例”（见2017年版的A.3）。

本文件修改采用ISO/IEC 9798-2:2019《信息安全技术　实体鉴别　第2部分：采用鉴别式加密的机制》。

本文件与ISO/IEC 9798-2:2019相比做了下述结构调整：

——4.1对应ISO/IEC 9798-2:2019的第4章，并增加了4.2；

——增加了附录D。

本文件与ISO/IEC 9798-2:2019的技术差异及其原因如下：

——关于规范性引用文件，本文件做了具有技术差异的调整，以适应我国的技术条件，调整情况集中反映在第2章“规范性引用文件”中，具体调整如下：

- 用规范性引用的GB/T 15843.1—2017替换了ISO/IEC 9798-1（见第3章），用规范性引用

的 GB/T 36624 替换了 ISO/IEC 19772(见第 3 章及第 6 章);

- 用规范性引用的 GB/T 16262(所有部分)替换了 ISO/IEC 8824(所有部分)(见附录 A);
- 增加了规范性引用 GB/T 25069—2022(见第 3 章);

——为保证与国家标准的协调一致,在“术语和定义”一章引导语增加了引用文件 GB/T 25069(见第 3 章);

——为保证与国家标准的协调一致,增加了“验证方”术语及定义(见第 3 章),删除了 ISO/IEC 9798-2:2019 的“密文”术语及定义;

——为保证文件的可读性,修改了符号“A,B”“I_U”“K_{UV}”“N_U”“R_U”“TN_U”“$Token_{UV}$”“T_U”“TVP_U”,增加了符号“IV”“R'_X”“$Text_n$”“$MUT.CR$”“$MUT.TS$”“$TTP.CR$”“$TTP.TS$”“$UNI.CR$”“$UNI.TS$”“$\|$”(见 4.1);

——为保持文本前后内容一致,保证文本的可读性,修改涉及在线可信第三方的机制标识符,将“$TP.TS$”更改为“$TTP.TS$”,将“$TP.CR$”更改为“$TTP.CR$”(见 4.1、第 8 章)。

本文件做了下列编辑性改动:

——根据国内实际情况,修改文件名称为“网络安全技术　实体鉴别　第 2 部分:采用鉴别式加密的机制”;

——删除了 ISO/IEC 9798-2:2019 第 1 章中对于附录 A 的说明,调整至第 5 章(见第 5 章);

——第 5 章增加了资料性引用的 GM/T 0078、GM/T 0103 及 GM/T 0105(见第 5 章);

——第 6 章用资料性引用的 GB/T 17901.1 替换了 ISO/IEC 11770-1(见第 6 章);

——增加了资料性附录“机制 $MUT.CR$——三次传递鉴别参考示例”(见附录 D)。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位:北京数字认证股份有限公司、中国电子技术标准化研究院、中国科学院大学、国家密码管理局、普华诚信信息技术有限公司、飞天诚信科技股份有限公司、格尔软件股份有限公司、浙江大华技术股份有限公司、陕西省信息化工程研究院、云南电网有限责任公司信息中心、北京时代亿信科技股份有限公司、郑州信大捷安信息技术股份有限公司、中国科学院软件研究所、公安部第三研究所、兴唐通信科技有限公司、北京信安世纪科技股份有限公司、长扬科技(北京)股份有限公司、北京时代新威信息技术有限公司、联通在线信息科技有限公司、中国科学院信息工程研究所、北京国脉信安科技有限公司、华为技术有限公司、鼎铉商用密码测评技术(深圳)有限公司、启明星辰信息技术集团股份有限公司。

本文件主要起草人:刘中、夏鲁宁、李彦峰、荆继武、王鹏、田敏求、林阳荟晨、王琼霄、郑亚杰、李向锋、王跃武、高五星、朱鹏飞、郑强、闫斌、赵晓荣、肖鹏、刘伟丰、刘为华、张立武、杨元原、蔡子凡、张宇、赵华、朱威儒、傅大鹏、颜雪薇、田学娟、郭丽芳、魏东、张振红、张严、程福兴、贾世杰、马原、袁峰、曾光、陈磊、许雪姣、李鑫、王新杰、梁斌、封维端、肖飞、陈萧宇。

本文件及其所代替文件的历次版本发布情况为:

——1997 年首次发布为 GB/T 15843.2—1997,2008 年第一次修订,2017 年第二次修订;

——本次为第三次修订。

引　言

GB/T 15843 旨在规范实体鉴别机制中不同种类的实体鉴别协议，拟由 6 个部分组成。

——第 1 部分：总则。目的在于规范实体鉴别机制中的鉴别模型和一般性约束要求。

——第 2 部分：采用鉴别式加密的机制。目的在于规范六种采用鉴别式加密实现实体鉴别的机制及相关要求。

——第 3 部分：采用数字签名技术的机制。目的在于规范十种基于数字签名技术的实体鉴别机制及相关要求。

——第 4 部分：采用密码校验函数的机制。目的在于规范四种采用密码校验函数的实体鉴别机制及相关要求。

——第 5 部分：使用零知识技术的机制。目的在于规范三种使用零知识技术的实体鉴别机制及相关要求。

——第 6 部分：采用人工数据传递的机制。目的在于规范八种在设备之间基于人工数据传递进行实体鉴别的机制及相关要求。

网络安全技术　实体鉴别
第2部分：采用鉴别式加密的机制

1　范围

本文件规定了两类（共六种）采用遵循GB/T 36624的鉴别式加密实现实体鉴别的机制。第一类不引入在线可信第三方，包含两种单向鉴别机制和两种相互鉴别机制。第二类引入一个在线可信第三方，包含两种单向或相互的实体鉴别机制。

本文件适用于指导基于鉴别式加密实现的实体鉴别系统、产品或服务的设计、开发和测试等。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 15843.1—2017　信息技术　安全技术　实体鉴别　第1部分：总则（ISO/IEC 9798-1：2010，IDT）

GB/T 16262（所有部分）　信息技术　抽象语法记法一（ASN.1）[ISO/IEC 8824（所有部分）]

注：GB/T 16262.1—2006　信息技术　抽象语法记法一（ASN.1）第1部分：基本记法规范（ISO/IEC 8824-1：2002，IDT）；

GB/T 16262.2—2006　信息技术　抽象语法记法一（ASN.1）　第2部分：信息客体规范（ISO/IEC 8824-2：2002，IDT）；

GB/T 16262.3—2006　信息技术　抽象语法记法一（ASN.1）　第3部分：约束规范（ISO/IEC 8824-3：2002，IDT）；

GB/T 16262.4—2006　信息技术　抽象语法记法一（ASN.1）　第4部分：ASN.1规范的参数化（ISO/IEC 8824-4：2002，IDT）。

GB/T 25069—2022　信息安全技术　术语

GB/T 36624　信息技术　安全技术　可鉴别的加密机制（GB/T 36624—2018，ISO/IEC 19772：2009，MOD）

3　术语和定义

GB/T 15843.1—2017、GB/T 25069—2022、GB/T 36624界定的以及下列术语和定义适用于本文件。

3.1

鉴别式加密　authenticated encryption

可逆的数据转换，这种数据转换利用密码算法产生数据的对应密文，未经授权实体无法在不被发现的情况下对其修改，同时提供了数据机密性、数据完整性与数据源鉴别。

注：本文件所定义的“鉴别式加密”，等同于GB/T 36624所定义的“可鉴别的加密”。

[来源：GB/T 25069—2022，3.298，有修改]